



**24/7 ATTACK
PREVENTION &
SAFEGUARDING
FOR EDUCATION**

censornet.

THE PLATFORM FOR COMPLETE SECURITY

Censornet's cyber security platform enables comprehensive monitoring and in-depth control of web, email and cloud application use to protect students from cyber-bullying, online radicalisation as well as inappropriate or malicious content – including viruses and other malware.



With over 15 years' experience in the education sector the Censornet platform includes numerous predefined template policies, rules and keyword dictionaries to simplify implementation and ensure rapid compliance with safeguarding guidelines.



Censornet specialise in providing true enterprise grade security at a price point accessible to schools, academies, colleges and Universities.

CYBER SECURITY MADE SIMPLE

Traditional security systems are being fast outpaced. We've built a security posture fit for today – and tomorrow – with identity at the heart. A new approach for the challenges of tomorrow.

Our email, web, and cloud application security works seamlessly with powerful identity management. Let them do their work – while you focus on strategic value.

Detailed analysis and reporting is available by time, user, device (hostname and MAC address), URL category, web category, cloud application class, cloud application name, cloud application action, keyword (e.g. filename, comment, etc.), policy name, risk level, email direction, delivery status (delivered, spam, virus, phishing, quarantined), outcome (block or allow).

Reports can be linked to schedules and sent via email as CSV, Excel Format or PDF attachments. Scheduling can also be used to provide regular email alerts to certain pupil actions, or the occurrence of specific keywords across email, web and cloud application use.

Whether audit data is required purely for visibility or for more formal proof of compliance with internal policies or external standards, regulations and legislation, the platform will provide the evidence needed.





INTELLIGENT WEB SECURITY

Censornet Web Security provides filtering of over 500 categories of web content covering billions of web pages. The solution includes both the Counter Terrorism Internet Referral Unit (CTIRU) (Prevent) and Internet Watch Foundation (IWF) illegal sexual content lists.

Advanced filtering enables educational establishments to comply with the UK Home Office Prevent strategy and the Counter Terrorism and Security Act 2015 and meet their duty to demonstrate "due regard to the need to prevent people from being drawn into terrorism".

- Different policies can be quickly and easily created for different ages or year groups
- Integrated with Microsoft® On-premise Active Directory (AD), Hybrid AD and Azure AD for simplified user and group policies
- Simple workflow for managing access to websites and responding to unblock requests (can be actioned by teachers, faculty or year heads, not just IT staff)
- Scheduled, Time Quota and Coaching access to site categories allows for more relaxed lunchtime and after-school policies
- Intelligent appropriate filtering ensures protection of pupils from harmful or inappropriate material without being overly restrictive or impacting on learning
- Specific categories that covers web security bypassing solutions such as proxy bypass sites or VPNs

Censornet Web Security also includes the ability to analyse web pages in real time for keywords and phrases that are associated with discrimination, bullying, self-harm, violence, grooming, radicalisation and extremism, with the convenience of pre-populated dictionaries. All dictionaries can be extended or customised if required.

Adverts within web pages can also be removed to protect young people from distracting or inappropriate brand messages, as well as malvertising which increasingly affects mainstream sites that aren't typically blocked.

SAFE SEARCH FOR SCHOOLS

Safe search can be enforced on popular internet search engines such as Google, Yahoo and Bing. Specific keywords or phrases can be blocked from being used in search strings. All searches are saved to provide an audit trail of which pupils searched for what terms or topics on the internet.



CLOUD APPLICATION SECURITY – GO BEYOND BLOCK AND ALLOW

Few websites today are entirely static. Most support a level of user interaction and are therefore applications, even if the site is a news site that simply allows users to comment on articles and stories.

Increasingly educational establishments need to implement granular policies that manage user actions within web applications. Simply blocking or allowing sites is no longer a viable solution that balances student protection with the need to learn.

Our Cloud Application Security provides visibility of all user activity within web or cloud applications, driven by an app catalogue that contains thousands of applications and thousands of user actions. If a web application is allowed, specific features within the application can be monitored or blocked. Using simple rules, sites can be made read-only. For example, monitoring and blocking comments with Facebook.

Keywords can be used to ensure that the content of messages, posts and tweets is appropriate and not derogatory to the organisation, or staff. Files uploaded to cloud storage applications – such as Dropbox, or Microsoft® OneDrive – can be scanned for content, risk words and malware.

ULTRAFAST AND UNOBTRUSIVE

Censornet uses a unique architecture that doesn't proxy all web traffic, ensuring an ultrafast and transparent experience that doesn't impact productivity or cause user frustration.

The Censornet Cloud is built on world-class infrastructure (including Amazon, Microsoft and IBM) in multiple locations for unparalleled speed, scalability and resilience. Personal data is regionalised to ensure local data protection and privacy requirements are met.





EMAIL SECURITY, ARCHIVING AND CONTINUITY

Censornet offer a comprehensive set of email security services from industry-leading protection from spam, phishing and malicious attachments, to solutions for sending email securely (encrypted email messaging), to archiving all email messages inbound and outbound, to providing an emergency inbox in the event that the primary mail provider suffers an outage to ensure continuous access to sent and received messages (until service is restored).

At the core of the Censornet Email Security (EMS) service is a powerful cloud-based mail routing engine that allows email administrators to control exactly how email flows in and out of the organisation. Multiple email providers can be supported, for example, so staff and students can use different email services (e.g Gmail, O365, Microsoft Exchange).

All aspects of inbound and outbound messages can be inspected – including headers, sender, recipient, subject, body, attachment type and size. Actions available include accept, reject, re-route, add content to subject/body/headers and quarantine based on message attributes and content.

Inbound and outbound emails can be analysed for keywords and phrases with customisable dictionaries specific to bullying, sexual content and obscenities/profanities.

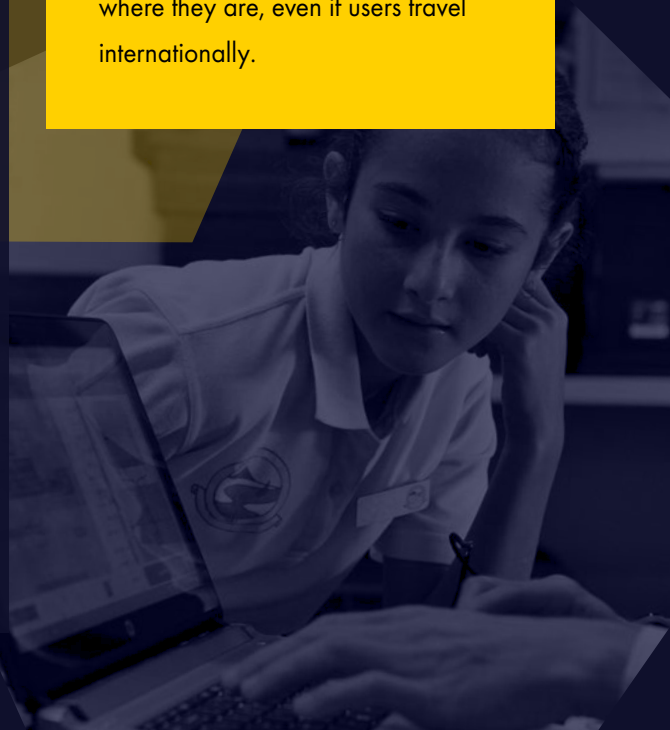
Censornet LinkScan rewrites all web links in emails and provides point-of-click protection from malicious or infected web pages, regardless of when a user clicks on the link – even months after a message was originally received.

It is clear more focus needs to be placed on security awareness training in the education sector in order to raise awareness of cyber security threats, reduce the risks associated with cyber attacks, and embed a culture of compliance.

PROTECTION INSIDE AND OUTSIDE THE CLASSROOM

Censornet uses a combination of gateways and agents to protect students on and off the network, regardless of the device used. Furthermore, the Censornet Cloud Gateway features a captive or guest portal to ensure rules and policies are applied when students use their own personal devices to access web-based resources inside and outside the classroom, supporting BYOD initiatives.

Agents for Windows and Mac OS X protect devices regardless of where they are, even if users travel internationally.





SECURITY AWARENESS TRAINING

According to IBM data, more than 90% of cyber-attacks are made possible because of human error. Strengthen your human firewall with Security Awareness Training from Censornet.

Our fully automated, computer-based training allows you to use threat and phishing simulations to train your staff to spot and avoid cyber-attacks. The results identify your high-risk users and provide clear action plans. You'll maintain full visibility and demonstrate clear ROI, with regular risk reports detailing the performance and vulnerabilities within your eco-system.

Developed with a Microsoft365 integration that will handle the management of your employees, you'll be able to deliver one of the best cyber security training programmes available in the market.

SAT provides a quick and cost-effective solution that can deliver benefits within hours of deploying. A simple, competitively priced commercial model provides all the content, simulations, reporting, implementation, support and feature upgrades in a single license.

TRANSFERRABLE SKILLS

More than 90% of attacks are result of human error. It's time to strengthen your human firewall.

Security Awareness Training builds knowledge in the education sector among administrators, faculty and teachers. You will be creating a cyber-safe culture, enabling transferable skills keeping your staff safe in and outside the workplace.

- ♥ Out of the box configuration allows for rapid, effective deployment without administrative burden
- ♥ Add-on package included if organisation has Microsoft 365 E5 or Microsoft Defender for Office 365 Plan 2, which includes threat investigation and response capabilities
- ♥ Fully SCORM compliant for users wanting to house content within their learning management system (LMS)
- ♥ Multi-lingual options – important for customers with multiple locations
- ♥ Automated delivery of simulations and training
- ♥ Automatic report and dashboard creation

ASE

GET FULL PROTECTION IN ONE SIMPLE PLATFORM

You need total visibility. Seamless authentication. Powerful intelligence.

Our platform does it all in one place. Integrated web, email, cloud, and identity. Stopping attacks before they take hold, 24/7.

Censornet shares advanced threat intel across email, web and cloud applications, synthesising a billion threats a day. Its autonomous security engine (ASE) is the brains behind the platform, working at lightning speed so you don't have to work like a robot.



24/7 cybersecurity

The rules-based engine works autonomously around the clock, with little to zero human input, meaning your people are freed from repetitive low-level tasks to make more strategic impact.



Protection across every attack surface

With genuine integration, the Censornet platform seamlessly actions automation between your web, email, and cloud application security, MFA and IDaaS for complete, uncompromised protection.



World-class threat intelligence

In-built threat intelligence feeds (usually reserved for big budgets) provide enterprise-level security to pro-actively stop attacks from entering the kill chain.

Platform Modules



Secure your entire organization from known, unknown & emerging email security threats - including email fraud.



Protect users from web-borne malware, offensive or inappropriate content & improve productivity.



Reduce impact of large scale data breaches by protecting user accounts with more than just passwords.



Defend against cybercriminals by strengthening your engaging and stimulating automated training.



Discover, analyze, secure & manage user interaction with cloud applications - inline & using APIs.



Automatically authenticate users with rich contextual data and enable complete identity-threat protection.

AUTONOMOUS SECURITY ENGINE

Enable traditionally silo'd services to share security context, state data and events whilst leveraging world class threat intelligence.



ASE provides 24x7 security so you don't need to.



Full access to threat intelligence without the cost.



Integral part of the Censornet platform.

Ready to transform your security into 24x7 protection?

Visit censornet.com
or call +44 (0) 845 230 9590